Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claims 1-44: (cancelled)

45. (new) A method for analyzing the security of an information system comprising:

a modelling phase, comprising on the one hand the specification of the architecture of the information system with a graphical representation of a set of components of the system and relations between said components, each component being associated with at least one state initialized with a sound value, the relations between two determined components comprising propagation relations able to convey attacks, and on the other hand the specification of a set of behavioural rules, from the standpoint of the operation of the system and from the standpoint of security, associated with the components of the system, each behavioural rule comprising one or more predicates and/or one or more actions; and,

a simulation phase, comprising the specification and the simulation of potential attacks against the information system, a successful attack causing a state of a component to pass to an unsound value.

46. (new) The method of claim 45, wherein, a name being associated with each component, one or more adjectives may also be associated with said component, which adjectives make it possible to designate said component without naming it.

47. (new) The method of Claim 45, wherein determined states are associated with each component of the information system, each state being able to take a sound value and one or more unsound values.

48. (new) The method of Claim 47, wherein certain at least of said states pertain respectively to the activity, the confidentiality, the integrity and/or the availability of the component with which they are associated.

49. (new) The method of Claim 45, wherein an alleged name may be associated with any determined component, in particular in the case where said determined component is a usurper.

50. (new) The method of Claim 45, wherein a link to another component may be associated with any determined component, in particular in the case where said determined component is usurped and where said other component is a usurper.

51. (new) The method of Claim 45, wherein the propagation relations are bidirectional relations able to convey attacks in both directions.

52. (new) The method of Claim 45, wherein the relations between any two determined components comprise service relations making it possible to designate a component on the basis of another component.

53. (new) The method of Claim 45, wherein the behavioural rules comprise rules for propagating attacks, these rules being for example implemented in components which are vectors of attacks, and rules for absorbing attacks, these rules being for example implemented in components which are the target of attacks.

54. (new) The method of Claim 45, wherein the behavioural rules comprise binary rules, for example Boolean logic conditions giving a value of type yes/no, and/or functional rules, for example logic conditions involving a routing action (for a propagation rule) or contagion action (for an absorption rule).

55. (new) The method of Claim 45 comprising, at the end of the modelling phase, the construction of a local routing table, making it possible to direct an attack from a start component to a finish component.

56. (new) The method of Claim 55, wherein the local routing table is generated automatically according to the principle of the shortest path between the start component and the finish component.

57. (new) The method of Claim 56, wherein the attacks simulation step comprises the updating of the state of a component of the system altered by a successful attack.

58. (new) The method of Claim 57, wherein the simulation phase furthermore comprises the building of a file or journal of the attacks, containing the log of the changes of the state of the components consequent upon successful attacks, in particular to allow subsequent processing by a user.

59. (new) The method of Claim 57, wherein the attacks comprise elementary attacks corresponding to unsound state values.

60. (new) The method of Claim 57, wherein the attacks further comprise a special usurping attack.

61. (new) The method of Claim 57, wherein an attack is defined, in particular, by a type of attack, a type of protocol, and attack path elements.

62. (new) The method of Claim 61, wherein the attack path elements comprise a start component, a finish component, a target component, and as appropriate one or more intermediate components.

63. (new) The method of Claim 61, wherein the list of components already traversed by an attack is saved in one or more upstream stacks.

64. (new) The method of Claim 63, wherein the upstream stacks comprise a stack containing the exhaustive list of all the components traversed, designated by their real name.

65 (new) The method of Claim 63, wherein the upstream stacks comprise a stack containing the list of only those components traversed which are opaque, designated by their real name or, as appropriate, by their alleged name.

66. (new) The method of Claim 61, wherein the list of destination components of an attack is saved in at least one downstream stack.

67. (new) The method of Claim 61, wherein the attacks are defined in a language using the same words as a language in which the behavioural rules are defined.

68. (new) The method of Claim 61, wherein the modelling phase and/or the simulation phase are implemented by a user by means of a man/machine interface comprising a multiview functionality, wherein a graphical representation of the system is presented to the user as several views.

69. (new) The method of Claim 68, wherein each view represents a subsystem of the system, which is relatively autonomous and independent of the remainder of the system.

70. (new) The method of Claim 68, wherein the function of interconnection between the components included in two distinct views is ensured only via the common component or the common components shared by the two views.

71. (new) The method of Claim 68, wherein the behavioural rules for the components belonging to a view do not call by name upon components belonging to another view.

72. (new) The method of Claim 68, wherein the views are associated with respective subsystems, for example of like level, which are interconnected together via at least one common component.

73. (new) The method of Claim 68, wherein a higher view is associated with the system as a whole, whereas one or more lower views are respectively associated with a determined subsystem of the system.

74. (new) The method of Claim 73, wherein a determined component, common to the higher view and to a determined lower view, represents the corresponding subsystem viewed from the system as a whole, and vice versa.

75. (new) The method of Claim 74, wherein said common component is the sole interface between the higher view and said determined lower view.

76. (new) The method of Claim 74, wherein the modelling phase further comprises the specification of one or more basic metrics associated respectively with the components.

77. (new) The method of Claim 76, wherein the basic metrics comprise a metric of effectiveness of parries, a metric of effectiveness of detection of attacks, and/or a metric of the means of an attacker.

78. (new) The method of Claim 76, wherein the simulation phase comprises the calculation of one or more metrics of probability of mishap.

79. (new) The method of Claim 78, wherein the metrics of probability of mishap comprise a metric of probability of passage of an attack on a component.

80. (new) The method of Claim 78, wherein the metric of probability of passage of an attack on a component is calculated according to the formula "probability of passage = (means of the attacker)/(effectiveness of the protection)".

81. (new) The method of Claim 78, wherein the metrics of probability of mishap comprise a metric of probability of nondetection of an attack on a component.

82. (new) The method of Claims 81, wherein the metric of probability of nondetection of an attack on a component is calculated according to the formula "probability of nondetection = (means of the attacker)/(effectiveness of the detection)".

83. (new) A device for the implementation of a method for analyzing the security of an information system, said device comprising:
a man/machine interface for the implementation of a modelling phase comprising a modelling phase, comprising on the one hand the specification of the architecture of the information system with a graphical representation of a set of components of the system and relations between said components, each component being associated with at least one state initialized with a sound value, the relations between two determined components comprising propagation relations able to convey attacks, and on the other hand the specification of a set of behavioural rules, from the standpoint of the operation of the system and from the standpoint of security, associated with the components of the system, each behavioural rule comprising one or more predicates and/or one or more actions; and,
an attacks/parries engine for a implementation of a simulation phase comprising the specification and the simulation of potential attacks against the information system, a successful attack causing a state of a component to pass to an unsound value.

84. (new) The device of Claim 83, wherein the man/machine interface has a functionality of multiview display of the system modelled.

85. (new) The device of Claim 83, wherein the man/machine interface is configured to display the system modelled according to a components/relations model.